КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ТОРГОВЕЛЬНО-ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
Факультет інформаційних технологій
Кафедра інженерії програмного забезпечення та кібербезпеки

СИЛАБУС (SYLLABUS)
Дисципліна «Безпека інформаційних систем і мереж/ Security of information systems and chains»

ІНФОРМАЦІЯ ПРО ВИКЛАДАЧА

Викладач	Пашорін Валерій Іванович
Науковий ступінь	Кандидат технічних наук
Вчене звання	Професор
Посада	Професор кафедри інженерії програмного забезпечення та кібербезпеки
Адреса кафедри	м.Київ, вул. Кіото 19, каб. Б-524, Б-531
E-mail	progen@ukr.net
Консультації	Відповідно до графіку індивідуальних консультацій на сайті кафедри

ПОЛІТИКА АКАДЕМІЧНОЇ ДОБРОЧЕСНОСТІ

https://knute.edu.ua/file/NjY4NQ==/bf27ad9293fa2bb6f9b2c3031d4b6e4a.pdf

Дотримання академічної доброчесності передбачає:

- самостійне виконання навчальних завдань, завдань поточного та підсумкового контролю результатів навчання (для осіб з особливими освітніми потребами ця вимога застосовується з урахуванням їхніх індивідуальних потреб і можливостей);
- посилання на джерела інформації у разі використання не авторських ідей, розробок, тверджень, відомостей і т.п.;
- дотримання норм законодавства про авторське право і суміжні права;
- надання достовірної інформації про результати власної наукової діяльності, використані методики досліджень і джерела інформації.

Порушенням академічної доброчесності вважається:

- академічний плагіат – оприлюднення (частково або повністю) наукових (творчих) результатів, отриманих іншими особами, як результатів власного дослідження (творчості) та/або відтворення опублікованих текстів (оприлюднених творів мистецтва) інших авторів без зазначення авторства;
- самоплагіат – оприлюднення (частково або повністю) власних раніше опублікованих наукових результатів як нових наукових результатів;
- фабрикація – вигадування даних чи фактів, що використовуються в наукових дослідженнях;
- фальсифікація – свідома зміна чи модифікація вже наявних даних, що стосуються наукових досліджень.

За порушення академічної доброчесності здобувачі освіти можуть бути притягнені до академічної відповідальності:

- повторне проходження оцінювання (модульний контроль, іспит, залік тощо);
- повторне проходження відповідного освітнього компонента освітньо-професійної програми;
- відрахування з Університету;
- позбавлення наданих університетом пільг;
- відмова у присудженні відповідного ступеня вищої освіти;

ПОЛІТИКА ЩОДО ВІДВІДУВАННЯ ЗАНЯТЬ

- відвідування занять є обов'язковим;
- Студент, який пропустив практичне заняття, самостійно вивчає матеріал (при виникненні питань може звертатися за консультацією згідно розкладу консультацій викладачів оприлюдненого на сайті кафедри) за наведеними джерелами, виконує завдання і здає його викладачу.
- за об'єктивних причин (наприклад, хвороба, міжнародне стажування та ін.) навчання може відбуватись в он-лайн формі за погодженням із викладачем дисципліни.

ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Назва дисципліни / тип дисципліни	Безпека інформаційних систем і мереж / вибіркова
Навчальний рік	2022-2023, 2023-2024
Факультет	Факультет інформаційних технологій
Курс	3-4
Семестр	6-8
Освітній ступінь	Бакалавр
Галузь знань	12 «Інформаційні технології»
Спеціальність	122 «Комп'ютерні науки»
Загальна характеристика	Кількість годин –180 Кількість кредитів – 6 **Види занять:** лекції, практичні, самостійна робота. **Співвідношення аудиторних годин і годин самостійної роботи** - 68/112 **Мова викладання** – українська **Форма викладання** – очна
Підсумковий контроль	Екзамен
Програмне забезпечення	ОС Windows
Обладнання	Проектор, комп'ютерна техніка із встановленим програмним забезпеченням та доступом до мережі Інтернет.
Необхідні попередні дисципліни	«Алгоритмізація та програмування», «Комп'ютерні технології обробки та візуалізації даних»
Методика вивчення	Методика вивчення дисципліни полягає у набутті студентами знань теоретичного і практично-прикладного характеру під час лекцій, лабораторних занять, самостійної роботи та вивчення першоджерел і навчально-методичної літератури.
Мета і завлання	**Метою** викладання дисципліни є формування теоретичних знань та практичних навичок, необхідних для ефективного використання інформаційних технологій в інформаційних системах і мережах а також запобігання розголошенню, витоку і неправомірному оволодінню інформацією, протиправним діям щодо знищення, модифікації, копіювання і блокування інформації. **Завдання** дисципліни полягають у тому, щоб ознайомити студентів із законодавчим, організаційним, інженерно-технічним і програмними рівнями безпеки інформаційних систем, засобами і методами управління контролем доступу в комп'ютерних системах, методами ідентифікації і аутентифікації користувачів і ресурсів інформаційних систем, особливостями захисту інформації в локальних і корпоративних мережах, навчити їх реалізовувати практично правила

	політики безпеки.
Місце дисципліни в освітньо-професійній програмі	
Фахові компетентності (результати навчання)	СК 14 Здатність застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти й експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об'єктів критичної інформаційної інфраструктури.
Програмні результати навчання	ПР 16 Розуміти концепцію інформаційної безпеки, принципи безпечного проектування програмного забезпечення, забезпечувати безпеку комп'ютерних мереж в умовах неповноти та невизначеності вихідних даних.

ТЕМАТИКА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Тема 1. Основні положення теорії інформаційної безпеки.

Основні терміни та визначення інформаційної безпеки. Актуальність інформаційної безпеки. Інформаційна безпека в умовах функціонування глобальних мереж. Цілі і завдання інформаційної безпеки. Види можливих порушень в роботі інформаційної системи. Розголошування. Витік інформації. Несанкціонований доступ до системи або мережі. Загрози інформації. Основні поняття і класифікація загроз. Основні загрози доступності. Основні загрози цілісності. Основні загрози конфіденційності. Порушники інформаційної безпеки. Класифікація порушників. Методика вторгнення. Умови, що сприяють неправомірному оволодінню інформацією. Канали витоку інформації та перехоплення даних. Модель безпеки: структура і компоненти. Засоби забезпечення безпеки інформаційних систем і мереж.

Тема 2. Правове забезпечення інформаційної безпеки.

Структура законодавства по захисту інформації. Основні нормативні керівні документи, що стосуються державної таємниці. Нормативно-довідкові документи. Призначення і завдання у сфері забезпечення інформаційної безпеки на рівні держави. Міжнародні стандарти інформаційної безпеки. Державний стандарт України із захисту інформації.

Тема 3. Адміністративне та організаційне забезпечення інформаційної безпеки.

Організаційний захист. Політика безпеки. Програма безпеки. Управління ризиками. Стандарти інформаційної безпеки. Критерії оцінювання захищеності інформаційної системи. «Критерії оцінки довірених комп'ютерних систем» («Помаранчева книга»). Міжнародний стандарт побудови ефективної системи безпеки ISO 17799. Аналіз засобів порушення інформаційної безпеки.

Тема 4. Програмно–технічне забезпечення інформаційної безпеки.

Інженерно-технічний рівень інформаційної безпеки. Технічні засоби для несанкціонованого доступу до інформації. Засоби протидії несанкціонованому доступу до інформації. Канали витоку інформації. Захист інформації від витоку по технічним каналам. Апаратні засоби захисту. Програмні засоби захисту. Ідентифікація і аутентифікація. Управління доступом. Реєстрація подій і аудит. Функціональне призначення та реалізація парольного захисту. Паролі в ОС Windows. Мережева аутентифікація в Windows. Апаратні засоби аутентифікації.

Тема 5. Основи криптографічного захисту інформації.

Основні терміни та поняття криптографії. Історія та законодавча база криптографії. Перші методи шифрування перестановки та заміни. Одноалфавітні системи шифрування Віженера, Плейфейра та інші. Багатоалфавітні системи шифрування: Бьюфорта, Віженера та інші. Сучасні криптосистеми та їх особливості. Основні типи алгоритмів шифрування. Електронний цифровий підпис. Управління ключами та сертифікація ключів. Стеганографічні методи захисту інформації.

Тема 6. Захист від руйнуючих програмних дій.

Поняття і класифікація комп'ютерних вірусів. Коротка характеристика вірусів. Програмні закладки. Програми - шпигуни і логічні бомби. Троянські програми. Черв'яки і інші шкідливі програми. Визначення видів захисту від вірусів. Антивірусні програми. Корпоративні антивіруси. Правила використання стороннього програмного забезпечення. Спам і засоби боротьби з ним.

Перелік навчальних робіт студентів та оцінки їх у балах з дисципліни «Безпека інформаційних систем і мереж»

Види робіт	К-сть балів
Практичне заняття №1. Тема: «Створення політики інформаційної безпеки для організації».	6
Практичне заняття №2. Тема: «Засоби несанкціонованого доступу до інформації».	6
Практичне заняття №3. Тема: «Методи і засоби технічного захисту інформації».	7
Практичне заняття №4, 5. Тема: «Парольний захист. Безпека зберігання даних в ОС Microsoft Windows».	10
Практичне заняття №6. Тема: «Дослідження та захист реєстру операційної системи Windows».	7
Практичне заняття №7. Тема: «Створення алгоритму криптографічного захисту».	7
Практичне заняття №8. Тема: «Дослідження системи захищеного електронного листування PGP».	7
Виконання індивідуального завдання (СР)	30
Разом: Аудиторна робота	**70**
Самостійна робота (СР)	**30**
Всього:	**100**

КОНТРОЛЬ ТА КРИТЕРІЇ ОЦІНЮВАННЯ ЗНАНЬ СТУДЕНТІВ

При вивченні дисципліни використовуються наступні форми контролю знань студентів: поточний; модульний; підсумковий.

Поточний контроль передбачає перевірку теоретичних питань, самостійної роботи, практичних робіт та усне опитування по кожній практичній роботі. По даному виду контролю оцінювання знань здійснюється у відповідності до бального розподілу наведеного в попередній таблиці.

Модульний контроль передбачає виконання модульної контрольної роботи. Всі завдання оцінюються в 20 балів. Перше завдання (теоретичне) – 4 бали, друге завдання (практичне) – 8 балів, третє завдання (практичне) – 8 балів.

Формою підсумкового контролю є екзамен. Екзаменаційна оцінка (100 балів) є результатом виконання двох теоретичних питань (2 х 20 балів = 40 балів) та практичного завдання (60 балів).

Результуюча оцінка з дисципліни визначається як середня від балів набраних протягом семестру та отриманих на іспиті.

СПИСОК РЕКОМЕНДОВАНИХ ДЖЕРЕЛ

Основний:

1. Положення про технічний захист інформації в Україні від 27 вересня 1999 року № 1229/99.
2. Остапов С.Е., Євсеєв С.П., Король О.Г., Технології захисту інформації – Чернівці.- Видавничий дом «Родовід», 2018. – 471с.
3. Кавун С.В. Інформаційна безпека. Харків : ХНЕУ, 2016. -213с.
4. Гончарова Л.Л., Возненко А.Д., Стасюк О.І., Коваль Ю.О. Основи захисту інформації в

телекомунікаційних та комп'ютерних мережах. – К., 2016. – 435с., іл.160.
5. Єсін В. І. Безпека інформаційних систем і технологій: навчальний посібник / В. І. Єсін, О. О. Кузнецов, Л. С. Сорока. – Х. ХНУ імені В. Н. Каразіна, 2017. – 632с.